

RE: File extensions spoofable in MSIE download dialog

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2001-11/0213.html>

From: Jonathan G. Lampe (jonathan@stdnet.com)

Date: 11/26/01

Message-Id: <5.1.0.14.0.20011126101415.00adccf0@mail.stdnet.com>
Date: Mon, 26 Nov 2001 12:00:21 -0600
To: bugtraq@securityfocus.com
From: "Jonathan G. Lampe" <jonathan@stdnet.com>
Subject: RE: File extensions spoofable in MSIE download dialog

I could not reproduce this problem with semi-current versions of the latest browsers.

In all instances where I attempted to force an executable, binary file across the wire in response to a request for a text file either:

- 1) an ASCII representation of the executable file was loaded into a notepad.exe (as a file with the usual ".log" extension would be)
- 2) I was asked by a dialog whether I wanted to open or save "gotcha.exe"

In no instance was I able to "silently" download and execute an executable in response to a request for a text file.

These are the two browsers I tested with:

IE 5.50.4522.1800 SP1, Q299618

IE 6.0.2600.0000 Update Q312461

Here's the ASP I tried to use to test this one.

(Adapted from one of Microsoft's recommendations on how to push binary files from

ASPs. <http://support.microsoft.com/support/kb/articles/q276/4/88.asp>)

I tried the following four variations in my test: (Comment/uncomment the lines!)

1. Bogus Content Type, No Attachment Header
2. octet Content Type, No Attachment Header
3. Bogus Content Type, Attachment Header
4. octet Content Type, Attachment Header

<%

Const adTypeBinary = 1

Dim strFilePath

Dim Name

SecurityFocus Bugtraq: RE: File extensions spoofable in MSIE do

```
Name = "gotcha.exe"
```

```
'Set the content type to the specific type that you are sending.
```

```
'Response.ContentType = "application/definitely-not-in-your-list"
```

```
Response.ContentType = "application/octet-stream"
```

```
'Response.AddHeader "Content-Disposition", "attachment; filename=" & Name  
& ""
```

```
strFilePath = Server.MapPath(".") & "\frhed.exe"
```

```
Response.Write strFilePath
```

```
Set objStream = Server.CreateObject("ADODB.Stream")
```

```
objStream.Open
```

```
objStream.Type = adTypeBinary
```

```
objStream.LoadFromFile strFilePath
```

```
Response.BinaryWrite objStream.Read
```

```
objStream.Close
```

```
Set objStream = Nothing
```

```
%>
```

Here's the .htm from which testing was initiated.

```
<html>
```

```
<head>
```

```
<title></title>
```

```
</head>
```

```
<body>
```

```
<p>This is a test</p>
```

```
<p>Click here for an .exe</p>
```

```
<p>Click here for a .txt</p>
```

```
<p>Click here for a .log</p>
```

```
<p>&nbsp;</p>
```

```
</body>
```

```
</html>
```

In addition, I set up a directory on an IIS server with the following files in it:

(BTW, frhed is the name of a great bin/hex editor – just the first exe I grabbed for testing!)

- frhed.htm

- frhed.txt (text file)

SecurityFocus Bugtraq: RE: File extensions spoofable in MSIE do

- frhed.exe (executable)
- frhed.log (ASP file as defined above)

Finally, I enabled the ".log" extension as an ".asp" extension clone.

Regards,

- Jonathan G. Lampe
- Standard Networks, Inc.
- 608.227.6100
- jonathan@stdnet.com

+=====

Other Info

My company had a usability issue with Microsoft Internet Explorer 5.0 and 5.5 which may be related to this behavior. (One of our web applications builds files on the fly when called. Early versions of IE 5.0/5.5 displayed and saved the filename of the "referring page" rather than the filename and contents we were trying to push down to the user with a function similar to the one above.) Our issue seemed to be magically resolved in an IE security rollup patch. (Go here – <http://www2.stdnet.com/sans/silocksupportbulletin01.pdf> – for more information on this.)

+=====

Original Report Follows

+=====

OVERVIEW

A flaw in Microsoft Internet Explorer allows a malicious website to spoof file extensions in the download dialog to make an executable program file look like a text, image, audio, or any other file. If the user chooses to open the file from its current location, the executable program will be run, circumventing Security Warning dialogs, and the attacker could gain control over the user's system.

A piece of HTML can be used to cause a normal download dialog to pop up. The dialog would prompt the user to choose whether he/she wants to "open this file from its current location" or "save this file to disk". The file name and extension may be anything the malicious website administrator (or a user having access there) wishes, e.g. README.TXT, index.html, or sample.wav. If the user chooses the first alternative, "open the file from its current location", an .EXE application is actually run without any further dialogs. This happens even if downloading a normal .EXE file from the server causes a Security Warning dialog.

The user has no way of detecting that the file is really an .EXE program and not a text, html, or other harmless file. The program could quietly backdoor or infect the user's system, and then pop up a window which does what the user expected, ie. show a text document or

SecurityFocus Bugtraq: RE: File extensions spoofable in MSIE do

play an audio file.

No active scripting is necessary in order to exploit the flaw. The malicious website can be referred e.g. in an iframe, in a normal link, or by javascript.

DETAILS

The flaw is in the way Internet Explorer processes certain kind of URLs and HTTP headers. No further technical details are disclosed this time, as there is no proper workaround and the vulnerability could be relatively easily and unnoticeably exploited to spread virii, install DDoS zombies or backdoors, format harddisks, and so on.

The flaw has been successfully exploited with Internet Explorer 5.5 and 6. An IE5 with the latest updates shows the spoofed file name and extension without a sign of EXE, and issue no Security Warning dialog after the file download dialog.

Internet Explorer 6 is exploitable in a slightly different way, but the effect is the same. The user gets a download dialog with the spoofed file name and extension, and can choose between "Open" and "Save". Opening the file causes the program to be run.

Older versions such as IE5.0 behave somewhat differently. The dialog indicates the user is about to execute an application; the dialog has the word "execute" instead of "open", and a Security Warning dialog appears after choosing "execute". It still shows the spoofed file name and extension instead of "EXE".

Any way to skip all dialogs, ie. to run an application without ANY dialog with this vulnerability has NOT been found. In all variations of the exploit there is always the normal file download dialog, but the following Security Warning dialog is skipped.

Technical details of the vulnerability will be revealed later.

WORKAROUNDS

Opening a file type previously considered safe, e.g. plain text or HTML file isn't safe with IE. Users of the browser should avoid opening files directly and save them to disk instead (if opening them is necessary at all). If this flaw is being exploited, the file save dialog will reveal that the file is actually an executable program. Dealing with files from an untrusted source isn't advisable anyway. Another workaround is switching to another browser such as Opera or Netscape which don't seem to have this vulnerability.

VENDOR STATUS

Microsoft was contacted on November 19th. The company doesn't currently consider this is a vulnerability; they say that the trust decision should be based on the file source and not type. The origin of the file, ie. the web server's hostname can't be spoofed with this flaw. It's not known whether a patch is going to be produced. Microsoft is currently investigating the issue.

--

Jouko Pynnonen Online Solutions Ltd Secure your Linux -
jouko@solutions.fi <http://www.solutions.fi> <http://www.secmo.com>

SecurityFocus Bugtraq: RE: File extensions spoofable in MSIE do

Original Report Above

- *Previous message:* [Larry W. Cashdollar: "Xitami Webserver stores admin password in clear text."](#)
- *Maybe in reply to:* [Jouko Pynnonen: "File extensions spoofable in MSIE download dialog"](#)
- *Next in thread:* [Jouko Pynnonen: "RE: File extensions spoofable in MSIE download dialog"](#)
- *Reply:* [Jouko Pynnonen: "RE: File extensions spoofable in MSIE download dialog"](#)
- *Messages sorted by:* [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)